

REMARKS

This Amendment is in response to the Office Action dated June 7, 2004. Claims 1-51 are pending in the present application. Claims 1-14 and 16-30 are rejected, and claim 15 is objected to. Claims 1, 5-9, 11-16, 27, and 30 have been changed, and claims 31-51 have been added by this amendment.

Claim Objections

The Examiner objected to claim 7 because of an informality, namely that it has two steps numbered "c1a." Claim 7 has been corrected accordingly, and Applicant requests that the objections be withdrawn.

Claim Rejections – 35 USC 102

The Examiner rejected claims 1, 2, 4, 5, 7, 16, 17, 19, 20, and 22 under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,463,537 to Tello. Applicant has amended the claims to clarify the invention.

The Examiner stated that the security system disclosed by Tello includes a security engine wherein it is determined if the security feature (a smart card) is installed at the beginning of the boot-up cycle, that the encryption algorithms are written in nonvolatile memory, and that this includes a public key algorithm, RSA, which has both a public and a private key.

However, claim 1 recites a method for booting up a computer system in a secure fashion that includes determining the presence of a security feature element that is installed within a housing of the computer system such that a cover to the housing is opened to remove the security feature element. Furthermore, a portion of the public key stored on the

security feature element is stored to a nonvolatile memory of the computer system, and an algorithm is utilized to determine the presence of the security feature element prior to a subsequent boot-up of the computer system, wherein additional authorization is required to be input to the computer system to boot up the computer system if the security feature element is not present and was previously present in the computer system.

Tello does not disclose or suggest providing a security feature element prior to boot-ups of a computer system, where the element is installed within a housing of the computer system such that a cover to the housing is opened to remove the security feature element, and if that security element is not present, additional authorization is required for boot-up of the computer, as recited in Applicant's claim 1. Rather, Tello discloses a security system in which a smart card is inserted by a user into a card reader 133 and smart card interface 135 (Fig. 1), which is detected by a security engine microprocessor 125 to determine access to the computer. The smart card inserted by the user is not installed within a housing of the computer system such that a cover to the housing is opened to remove the security feature element, as recited in claim 1. Furthermore, Tello describes security system electronics, including microprocessor 125, which are incorporated into the design of a standard motherboard to produce a security motherboard (col. 6, lines 15-20). Thus, Tello's security electronics can not be removed from the computer without preventing the computer from functioning, and therefore Tello's security system electronics are not a security feature element that can ever be removed or "not present," once they are detected to be previously present, as recited by Applicant's claim 1 to require authorization for boot-up. Removal (i.e., lack of presence after being previously present) of security system electronics is never contemplated or suggested by Tello, nor is such removal part of Tello's security features; and

Tello's smart card is not an installed security feature element as recited in claim 1. Tello therefore does not disclose or suggest the invention of Applicant's claim 1.

Claims 2, 4, 5, and 7 are dependent on claim 1 and are patentable for at least the same reasons as claim 1, and for additional reasons. For example, claim 7 recites determining whether a security feature element was previously present in the computer system if the security feature element is not present; Tello does not disclose or suggest any installed security features, within a computer's housing, which is not present but for which a previous presence is determined.

Claim 16 recites a system for booting up a compute in a secure fashion, and includes elements that perform functions similar to those recited in claim 1, including a security feature element installed in the computer system housing and requiring additional authorization if the security feature element is not present. Claim 16 is therefore believed patentable over Tello. Claims 17, 19, 20, and 22 are dependent on claim 16 and are believed patentable over Tello for at least the same reasons as claim 16, and for additional reasons as explained above for claims 2, 4, 5, and 7.

In view of the foregoing, Applicant believes that claims 1, 2, 4, 5, 7, 16, 17, 19, 20, and 22 are patentable over Tello, and respectfully requests that the rejection under 35 U.S.C. 102 be withdrawn.

Claim Rejections – 35 USC 103

The Examiner rejected claims 3, 6, 8-14, 18, 21, and 23-30 under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,463,537 to Tello as applied to claims 2, 5, and

above, and further in view of U.S. Patent No. 4,593,384 to Kleijne. Applicant has amended the claims to clarify the invention.

Claims 3, 6, 8-14 are dependent on claim 1, and claims 18, 21, and 23-30 are dependent on claim 16. Claims 1 and 16 are patentable over Tello as explained above. Kleijne also does not disclose or suggest providing a security feature element that is installed in computer system housing, and which can be removed and detected as removed after it was previously present, as recited in claim 1. Kleijne's security device destroys data in memory if a tampering event has been detected, and there is no detection of removal of the Kleijne's security device from a computer system. Claims 1 and 16 are therefore patentable over Tello in view of Kleijne.

Dependent claims 3, 6, 8-14, 18, 21, and 23-30 are patentable for at least the same reasons as claims 1 and 16, and for additional reasons. For example, claims 11 and 26 recite that it is determined whether the security feature element is an added feature of the computer system based on a previous POST sequence, if subjected to a tamper event. Neither Tello and Kleijne disclose or suggest checking, if a tamper event has occurred, whether a security feature has been added. Claims 12 and 27 recite that the portion of the public key stored in memory of the computer system, from previously-installed security elements, is cleared if the security feature element is a newly added feature (see Applicant's specification, page 8, lines 5-11); neither Tello or Kleijne disclose or suggest clearing keys provided from previously installed security features—in Tello and Kleijne, no keys can have been used before the security system was installed.

In view of the foregoing, Applicant believes that claims 3, 6, 8-14, 18, 21, and 23-30 are patentable over Tello in view of Kleijne, and respectfully requests that the rejection under 35 U.S.C. 103 be withdrawn.

Applicant has added claims 31-51. Claims 31 and 33 are dependent from claims 1 and 16, respectively, and recite that the security feature element is a security card installed in a slot of a system board in the computer system, as disclosed in Applicant's specification on page 6, lines 11-22 and in Fig. 3, and is patentable for at least the same reasons as claims 1 and 16.

Claims 32 and 34 are dependent on claims 1 and 16, respectively, and recite that the tamper event includes the cover of the housing of the computer system having been opened, as described in Applicant's specification on page 8, line 1, and is patentable over Tello and Kleijne for the same reasons as claims 1 and 16, and for additional reasons; e.g., Tello and Kleijne do not disclose this type of tamper event.

Claim 35 recites a method for booting up a computer system in a secure fashion, including determining a presence of a security feature element and storing a public key to computer memory, and upon and prior to subsequent boot-ups, determining the presence of the security feature element, determining whether the computer and element have been subjected to a tamper event, determining whether the same security feature element was present previously in the computer system, and allowing the computer system to be booted up if the security feature element is present, if the computer system has been subjected to a tamper event, and if the same security feature element is determined to have been previously present (Applicant's specification, page 8).

Tello and Kleijne do not disclose or suggest this invention. For example, neither

Tello or Kleijne disclose or suggest allowing a boot-up of a computer if a tampering has been detected, and if the same security feature element was present in the previous boot-up of the computer system. Tello does not check for the presence of a smart card in a previous boot up of the computer system. In col. 23, lines 43-52, Tello discloses checking if the security system has previously been set up, and if it was set up, waiting for a smart card insertion (col. 23, lines 53-55). Tello does not check if the same smart card was previously present, and does not allow the computer to boot if the same security electronic system was previously installed (Tello waits for a smart card). Thus, this is not the same as allowing a computer to boot if the same security element was found to previously present as in Applicant's claim 35. Kleijne also does not disclose or suggest detecting previous presence of his security memory device to allow boot-up. Applicant therefore believes that claim 35 is patentable over Tello in view of Kleijne. Claims 36-47 are dependent on claim 35 and are patentable for at least the same reasons as claim 35, and for additional reasons, such as similar reasons discussed above for similar dependent claims.

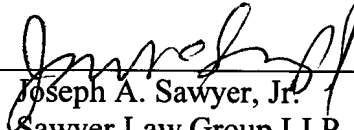
Allowable Claims

The Examiner stated that claim 15 would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. Applicant has added claim 48, which includes the subject matter of claim 15 and claims upon which it depends. Claims 49-51 are dependent on claim 48 and are therefore patentable for at least the same reasons as claim 48. Applicant therefore respectfully requests the allowance of claims 48-51.

In view of the foregoing, Applicants' attorney believes that this application is in condition for allowance. Should any unresolved issues remain, Examiner is invited to call Applicants' attorney at the telephone number indicated below.

Respectfully submitted,

September 8, 2004



Joseph A. Sawyer, Jr.
Sawyer Law Group LLP
Attorney for Applicant
Reg. No. 30,801
(650) 493-4540